AU/AWC/128/1999-04

AIR WAR COLLEGE

AIR UNIVERSITY

MILITARY DEPENDENCE ON COMMERCIAL SATELLITE COMMUNICATIONS SYSTEMS – STRENGTH OR VULNERABILITY?

by

Jack A. Hook, Jr., Colonel, U.S. Army

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel Victor Budura

Maxwell Air Force Base, Alabama

April 1999

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Tables

Page

Preface

This report examines the explosion of commercial satellite communications capabilities and the potential impact of these new capabilities on the Department of Defense. During my time on the Army Staff, this was a frequent topic of high interest for the Chief of Staff of the Army. The report is written for a general audience in relatively non-technical language, and requires very little prior understanding of satellite communications.

I would like to acknowledge the invaluable guidance and assistance of Colonel Vic Budura of the Air War College faculty in the preparation of this report. As the research advisor for this project, his suggestions on resources and references and his review of drafts added great value to the final product.

Abstract

The military's growing dependence on commercial satellite communications systems will become a strength or vulnerability based on how well the right balance is achieved between commercial and military systems. Determining that balance is a function of *clearly understanding* both DoD's requirements and the vulnerabilities and risks associated with the use of, and dependence on, commercial systems.

This report provides a short overview of the emerging commercial capabilities and then examines in depth the DoD process for validating requirements, the validated MILSATCOM requirements documented through that process, and the risks and vulnerabilities associated with the use of, and dependence on, commercial satellite communications systems.

The main conclusion drawn is that commercial capabilities can help satisfy DoD requirements for capacity, but at a "cost" in most cases of accepting risk with respect to several key qualitative requirements, especially with respect to protection, assured access, and control. A few additional conclusions are drawn about how to achieve the best balance to satisfy DoD requirements with the least amount of risk and cost.

Chapter 1

Introduction

Background

Commercial spending on space activities eclipsed government spending for the first time in 1996. With commercial space activities growing at 20 percent per year compared to 2 percent annual growth for government space programs, the trend will only continue. By 2001 industry expenditures are anticipated to climb to $117 billion, dwarfing the Department of Defense (DoD) space budget.[1] Much has been written about this explosion of new commercial systems and services. In the communications area, most writings have focused on the exciting capabilities the commercial sector is bringing into this new information-based world: Iridium's global cellular phone network and Teledesic's "Internet in the Sky," for example. At the same time, it is no secret that the military is becoming increasingly dependent on commercial systems. A key concern has arisen that our dependence has become a significant national vulnerability.

Scope

Most of the analysis to be done in this paper is equally applicable to all space functional areas.[2] The scope here will be limited to assessing the appropriate role of commercial satellite communications systems within the DoD military satellite communications (MILSATCOM) architecture.

Thesis

The military's growing dependence on commercial systems will become a strength or vulnerability based on how well the right balance is achieved between commercial and military systems, and determining that balance is a function of *clearly understanding* both DoD's requirements and the vulnerabilities and risks associated with the use of, and dependence on, commercial systems.

Methodology

After a short overview of the emerging commercial capabilities (Chapter 2), the DoD process for validating requirements and the validated MILSATCOM requirements documented through that process will be closely examined (Chapter 3). This will be followed by an in-depth look at the risks and vulnerabilities associated with the use of, and dependence on, commercial satellite communications systems (Chapter 4). Finally, some conclusions are drawn about how to achieve the right balance that can satisfy DoD requirements with the least amount of risk and cost.

Notes

[1] Gen (Ret) Thomas Moorman, quoted in Robert Holzer, "Officials See U.S. Military Role as Commercial Space Protector," *Defense News*, 30 November 1998. page?)

[2] For example, "Sentinals Rising," by LtCol Larry Grundhauser, published in the Winter 1998 *Airpower Journal* (pp. 61-80), is a similar assessment of capability versus vulnerability in the area of commercial satellite imagery.

Chapter 2

Commercial Satellite Communications Systems – Capabilities

The explosive pace of growth in the number of commercial satellite communications systems would have been unimaginable just a few years ago. More than one thousand commercial communications satellites, representing over thirty-five systems and networks, are projected to be in orbit within the next few years.[1] These new commercial satellite communications systems provide different capabilities and cover different areas of the earth in order to provide appropriate services to the markets their parent companies intend to target. Before discussing the capabilities and potential benefits of these various systems, it would be useful to first understand something about the different orbits they will occupy, since they are frequently referred to in this context.

Orbits

Current and emerging systems will be in orbits that span the range from Low Earth Orbit ("LEO"—altitudes up to about 1500 km) to Medium Earth Orbit ("MEO" – altitudes from about 5,000 to 15,000 km) to Geostationary Earth Orbit ("GEO" – altitude around 36,000 km).[2] GEO satellite systems offer the advantages of greater coverage of the earth, due to their high altitude, and simpler earth transceivers since they maintain a fixed position relative to the rotating earth below. But these advantages are offset by many other factors, such as higher launch costs to boost satellites into this significantly higher orbit, and time delays ("latency") for communications signals between the earth and the far distant satellite. LEO satellites are cheaper to place in orbit and have less latency, but their low altitude necessitates larger constellations (more satellites) to provide comparable earth coverage. MEO systems tend to offer a middle ground or compromise between the GEO and LEO systems with respect to the tradeoffs between constellation size, latency, and other factors, such as power requirements and antenna size.

LEO constellations have been further differentiated by industry as "little," "big," or "mega," based on the types of services provided by the system. "Little LEO" refers to constellations that provide primarily delayed "store and forward" communications for such applications as meter reading, paging, and messaging services. The term "Big LEO" is used to refer to constellations providing primarily real-time voice and some data communications. "Mega LEO" constellations (also referred to as "Broadband LEO"), provide real-time data communications for computer networks (such as Teledesic's "Internet in the Sky"), as well as voice communications.[3]

Capabilities

There are many differences in capabilities among the emerging commercial satellite communications systems, and as many ways to differentiate these capabilities. In order to assess military utility, some of the most useful distinctions are: when the system will be available ("Availability"); the volume of information the system can handle ("Capacity"); in what portions of the earth the system can be used ("Coverage"); and what applications the system will provide to the user ("Services").[4]

Availability

Many new networks, such as Inmarsat, Iridium, and others, are already operational. Many of the remainder are due to come on line at various times between now and 2002. Others are in various states of development, licensing, approval of orbital slots, and scheduling of launches, and thus have uncertain dates for full operational capability.

Capacity

Commercial satellite communications systems can also be differentiated with respect to capacity, or "throughput"—the amount of information that can be passed through the system. "Narrowband" systems encompass data rates of less than 64 kilobits per second (kbps), while "wideband" (also referred to as "broadband") systems encompass data rates greater than 64 kbps.[5]

Most of the "Big LEO" and "Little LEO" systems are narrowband low data rate systems for applications such as paging, voice, and short data and voice messaging. Examples include the ORBCOMM, Globalstar, and Iridium systems, which offer data rates of .3 to 2.4 kbps, 2.4 to 9.6 kbps, and 2.4 kbps, respectively.

Greater throughput enables wideband systems to support such applications as video and networking, including internet access. In addition to the "Broadband LEO" systems, some GEO systems also provide wideband throughput. Examples of broadband LEO systems include Teledesic (2 megabit per second (Mbps) uplink, 64 Mbps downlink) and SkyBridge (2 Mbps uplink, 20 Mbps downlink). Examples of GEO wideband systems include Spaceway (up to 6 Mbps), Astrolink (up to 9.6 Mbps), and GE*Star (up to 40 Mbps).

Coverage

Many of the new networks will provide regional coverage of some portion of the earth. Some will provide worldwide coverage of the entire globe.

Most of the regional systems are provided by one or two GEO satellites that appear to remain “stationary” over fixed portions of the earth. Examples of single GEO satellite systems providing regional coverage include Phase 1 of the ACTEL system, covering southern Africa (Zimbabwe, Zambia, Botswana, Namibia, and Mozambique); the AFRICOM system, covering the sub-Saharan Africa; the M2A system, covering a portion of the Asia-Pacific region, primarily Indonesia; and the MSAT system, covering North and Central America. Dual GEO systems cover larger regions. Examples include the AceS system, covering southeast Asia, India, China, and Australia; the OPTUS system, covering Australia, Papua/New Guinea, New Zealand, and Indonesia; the AMSC system, covering the United States, Mexico, and the Caribbean; and the ASC system, covering most of Asia (54 countries, from Turkey to Singapore east-to-west, and from Russia to Sri Lanka north-to-south).

Systems providing worldwide coverage are being launched into all three types of orbits. GEO constellations providing worldwide coverage include the ASTROLINK and INMARSAT systems, each consisting of five GEO satellites. The ICO system is a MEO constellation consisting of ten satellites providing worldwide coverage. LEO constellations providing worldwide coverage include the FAISAT, GEMnet, Iridium, Leo-One, Orbcomm, SkyBridge, Teledesic, and VITAsat systems.

Services

Services provided by the new commercial satellite communications networks include both voice and data. Applications range from paging to mobile and fixed voice services, video, facsimile, electronic mail, data messaging, short message service, position and timing using the Global Positioning System (GPS), and broadband services including high-speed multimedia data services and internet access.

Appendix A summarizes the capabilities and services of all "known" (filed with the Federal Communications Commission) commercial satellite communications systems currently operating or planned to be operational within the next few years. Appendix B identifies the shareholders and strategic partners, and the marketing strategies for each venture.[6]

Competition and Consolidation

A review of Appendices A and B reveals that there is a tremendous amount of competition for various markets and types of services. (For example, Globalstar is in direct competition with Iridium for customers who desire worldwide "Big-LEO" services of voice, data, fax, and paging.) This competition will inevitably produce winners and losers. That is, not all ventures will survive the competition, and new competitors will continue to enter. Some industry experts go so far as to characterize the developing competition as a pending "industry bloodbath."[7] As an example, if Appendix A were compiled just one year ago, it would have included such ventures as EUROSKYWAY, GE Starsys, QuasiGeo, and Odyssey, all of which have been cancelled since that time. It would not have included Cyprus GEM, Rostelesat, or WEST. No one can predict perfectly who will be added and deleted by this time next year.

Some of the larger well established satellite companies are involved in more than one venture, and are competing for several markets. Loral, for example, is a shareholder and/or partner in the Cyberstar, Globalstar, Movisat, and Skybridge systems. Hughes, Lockheed Martin, and Alcatel are also each involved in at least three systems.

There will also be consolidations. For example, the Millennium and M-Star projects were incorporated into Motorola's Celestri project. Then, on 21 May 1998, Motorola formed a partnership with Teledesic, Boeing, and Matra Marconi Space, and the Celestri project (and Millennium and M-Star) has been incorporated into the Teledesic project. Additional consolidations are likely.

Potential Benefits to the Department of Defense

The extent to which the military can benefit from this rapidly growing availability of commercial space-based communications systems has been a matter of intense debate in recent years. Some experts see the opportunity to help fill a rapidly growing defense bandwidth gap.[8] One predicts that early in the next century "dedicated military communications satellite systems will have disappeared."[9] Defense Department use of commercial satellite services to augment existing military systems "is growing rapidly," according to the deputy director for operations at the Defense Information Systems Agency.[10] The Department of Defense (DoD) expects to invest between $7 billion and $9 billion in satellite communications early in the next decade, and while some portion must be military owned and operated to meet many DoD requirements, officials expect the DoD system to rely heavily on commercial providers.[11] But to assess the true utility of commercial satellite communications systems to the military, it is first necessary to look more closely at DoD requirements, and the vulnerabilities and risks associated with the use of commercial satellite communications systems to meet those requirements.

Notes

[1] This estimate is reached by adding satellite quantities from known systems in the *Analysis Satellite Communications Database*, available at http://www.analysys.com/products/satellite/database.htm. This estimate tracks closely with launch industry projections identified by the Federal Aviation Administration in their *1997 LEO Commercial Market Projections*, 25 July 1997, Figure 5, p.7.

[2] Donald J. Dichman, "The Constellations in LEO," *Launchspace*, Aug/Sep 1997, 40-41.

[3] Ibid, 32.

[4] Data on the various commercial SATCOM systems identified throughout the remainder of this section is all drawn from the *Analysis Satellite Communications Database*.

[5] TRADOC Systems Manager for Satellite Communications, *The Army Satellite Communications (SATCOM) Architecture,* December 1998, E-3.

[6] Data for these two tables was compiled from *Analysis Satellite Communications Database*.

[7] Christy Hudgins-Bonafield, "Networking in the 21st Century," *Network Computing*, 15 March 1998, n.p.; on-line, Internet, 18 January 1999, available from http://www.techweb.com/se/directlink.cgi?nwc19980315s0017.

[8] Lt Danelle Barrett, "Commercial Satellite Constellation Offers Potential Military Benfits," *Signal*, November 1998, 43.

[9] Artur Knoth, "Space-Based Comms in the 21st Century," *International Defense Review*, May 1995, 63.

[10] BG James R. Beale, quoted in Pamela Houghtailing, "Agencies Eye Commercial Birds as Interest in Satellites Grows," *Federal Computer Weekly*, November 11, 1996, n.p.; on-line, Internet, 18 January 1999, available from http://www.fcw.com/pubs/fcw/1111/feat.htm.

[11] Ibid.

Chapter 3

Department of Defense Satellite Communications Requirements

The Department of Defense (DoD) requirements for satellite communications are rapidly growing. The first section of this chapter will examine some of the reasons for this. Then we will examine the processes by which DoD requirements are validated, and what those validated requirements are, in order to assess the extent to which commercial satellite communications systems may be able to satisfy DoD requirements.

Increasing Requirements

Within the DoD, the user community (e.g., regional Commanders in Chief—"CINCs," and other commanders of warfighting organizations) bears the primary responsibility for defining requirements. While the materiel development and combat development communities generally publish the formal requirements documents, these documents are only useful to the extent that they are based on valid input collected from users.

Generally, DoD users should identify their communications requirements in terms of the connectivity needed, not necessarily the means. That is, the user's basic requirement is for so much capacity of certain quality between point A and point B, without regard for whether the connectivity is provided by terrestrial or satellite systems. But as the relationship between technology, strategy, and the nature of combat has evolved in recent years, the number of communications requirements that can only be satisfied by space-based systems has grown dramatically.

Our National Military Strategy has shifted from an emphasis on forward-deployed forces towards a strategy based on the ability to project force from the continental United States. New technologies have enabled vast reductions in force structure, as smaller forces are capable of increased lethality, in no small part due to the application of information systems for increased situational awareness and improved weapons accuracy. Sensors and shooters are operating over greater distances not always supportable by terrestrial communications links. In addition to the increased requirements for transoceanic "reachback" communications capability to support split-based operations and force projection from the continental United States, deployed forces themselves are often much more dispersed within their theater of operations.

All of these changes in the way we fight have resulted in two significant impacts on DoD communications requirements. First, it has greatly increased our quantitative requirements for information systems and communications to link them. Second, with respect to means, it has significantly shifted the balance away from terrestrial systems and towards satellite communications systems. Cable and line-of-sight radio systems "remain vital capabilities, but they are not always well suited to satisfying the information needs of mobile, dispersed warfighters in high op-tempo, fluid mission environments."[1]

Requirements Validation Process

There are two dimensions to the satellite communications requirements that DoD users identify. These can be thought of as *quantitative* and *qualitative*. Quantitatively, users are concerned with how much *capacity* is needed, both in terms of the number of subscribers that must be supported in a network and the total throughput required between various nodes in the network. Qualitatively, users are concerned with specific characteristics of the voice and data traversing the network, and required characteristics of the system or network as a whole. Qualitative requirements address issues such as coverage, protection, survivability, control, security, "ruggedization," interoperability, and many others.

There are two distinct processes for validating these two types of requirements. The Joint Staff, as the primary user advocate, plays the key role in both processes.

Quantitative Requirements

As the quantitative requirements for satellite communications have been growing exponentially, existing military systems have not been able to keep pace with the increased demand. Military satellite communications (MILSATCOM) systems are thus managed as a scarce resource. To assist in its management of MILSATCOM resources the DoD maintains two databases. The Integrated Communications DataBase (ICDB) is an aggregation of all *current* satellite and terrestrial communications requirements. The Emerging Requirements Database (ERDB) identifies all projected *future* satellite communications requirements.

The ICDB is managed by the Joint Staff and maintained by the Defense Information Systems Agency (DISA). The Joint Staff manages the ICDB and validates requirements through the Joint MILSATCOM Panel (JMP) process. The JMP is chaired by a designated representative of the Joint Staff J6, and is made up of representatives from all the Services.[2] The panel forwards its recommendations to the Chairman, Joint Chiefs of Staff (CJCS), for final approval. Every user that plans to use satellites to communicate must have an ICDB number in order to compete for access to MILSATCOM resources. This includes not only DoD users, but many non-DoD users as well, such as the Department of State and national intelligence agencies. Non-DoD users submit their requirements to the Joint Staff through the Office of the Secretary of Defense (via the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence).

The ICDB currently contains approximately 3,000 validated satellite communications requirements and 55,000 validated terrestrial communications requirements.[3] Note that obtaining an ICDB number is a necessary but not a sufficient condition for a user to gain satellite access. Entry into the ICDB simply indicates that the requirement has been validated and approved by the CJCS. Since there are many more validated requirements than can be satisfied by existing systems, not everyone with an ICDB number will obtain access to MILSATCOM.

Actual allocation is based on a priority system, also managed by the Joint Staff, in accordance with JCS Memorandum of Policy 37 (currently under revision). Several factors are used to determine the priority of a validated requirement. These include the criticality of the requirement based on the function it supports (e.g., command and control, intelligence, logistics, or administrative), the Operations Plan or Operations Order being supported, and the mission impact of either not providing access or satisfying the requirement by some alternative communications means. The DoD MILSATCOM program exists primarily to support word wide core *command and control* communications services to the National Command Authority and the regional CINCs.[4] Thus these requirements are provided the highest priority. Since requirements, resources, and the world situation are constantly changing, Joint Staff policy directs a complete revalidation of all requirements contained in the ICDB every two years.[5]

Unlike the ICDB, the ERDB consists solely of satellite communications requirements and does not include terrestrial communications requirements. Also, the ERDB is not used to prioritize allocations or access. As concepts are developed and refined and technology progresses, ERDB requirements may or may not transition to become ICDB requirements. Those that do become ICDB requirements are then prioritized at that point.[6]

Qualitative Requirements

When identifying qualitative requirements, the whole system (including the user, space, and link segments, as well as the control system) must usually be considered. For example, it would not make sense to identify a requirement to protect only user equipment against the effects of high altitude electromagnetic pulse (HEMP). If HEMP is a risk, then the entire circuit path must be protected from end to end.

As with quantitative requirements, the user provides the primary input for defining qualitative requirements and the Joint Staff is the validating authority. Whereas the JMP is the Joint Staff’s validating body for quantitative requirements, the Joint Requirements Oversight Council (JROC) represents the CJCS for validating qualitative requirements.

The JROC is chaired by the Vice-Chairman of the Joint Chiefs of Staff (VCJCS) and composed by the vice-chiefs of each of the Services.

Generally, when any DoD service or agency identifies a functional shortcoming or need, they will submit a formal request to the JROC, in the form of a Mission Needs Statement (MNS), seeking authority to begin defining requirements and exploring different technical concepts to satisfy the mission need. If the JROC approves the MNS and it is determined that a materiel solution is necessary, then an Operational Requirements Document (ORD) is developed by the appropriate combat developer describing the operational capabilities needed to satisfy the mission need. If a MNS is likely to lead to several ORDs, as in the case of a broad mission area such as MILSATCOM, a Capstone Requirements Document (CRD) may be published in order to set common standards and requirements across the mission area. The CRD ensures any materiel fielded under the various ORDs is interoperable and maximizes the use of common resources.[7]

In the area of MILSATCOM, the JROC approved a MNS in April 1996.[8] This MNS represented the first time DoD had collected all MILSATCOM needs into a single document. As such, the JROC directed US Space Command to develop a CRD in order to adequately bridge the MNS to the set of system ORDs and plans for use of commercial services that collectively would meet the needs identified in the MNS well into the 21st century.[9] The JROC approved the MILSATCOM CRD and validated its capstone key performance parameters (KPP) on 6 April 1998.

Validated DoD Requirements

Required System Characteristics

The Department of Defense Advanced Military Satellite Communications Capstone Requirements Document (DoD MILSATCOM CRD) identifies seven required system characteristics for the MILSATCOM systems that will be designed and fielded to satisfy the MILSATCOM Mission Needs Statement: *coverage, capacity, protection, access and control, interoperability, flexibility, and quality of service*. Subordinate to these required system characteristics are dozens of quantitative and qualitative requirements. Each of the Operational Requirements Documents that will be developed under the CRD will identify dozens more requirements for their respective systems.

The CRD also addresses other considerations and requirements for *affordability* and for *transition* from legacy to new systems, to include requirements for *replenishment* of legacy constellations, *continuity of operations*, *backward compatibility*, and *synchronization* of MILSATCOM systems modernization and replenishment.[10]

Key Performance Parameters

Requirements documents generally distinguish those key requirements considered the most vital for supporting the future DoD warfighting vision. These requirements are called "Key Performance Parameters" (KPP). In recent years it has become common, due to affordability constraints, to identify both "threshold" and "objective" requirements. Threshold requirements represent the minimum acceptable standard and must be satisfied regardless of affordability. Objective requirements represent the ultimate desired capability, but fulfillment of the objective requirement may be deferred based on affordability criteria. The MILSATCOM CRD identifies several KPP, all of which fall under the first five of the seven required system characteristics identified above (coverage, capacity, protection, access and control, and interoperability). Because of their importance and fundamental nature, the threshold and objective requirements for these KPP warrant more detailed discussion.

Coverage. Because of the mobility of much of the DoD user population and the requirement to communicate in-transit to theaters of operations anywhere in the world, the DoD basically requires global coverage for its communications systems. Thus the objective requirement for the *coverage* KPP is the "ability to provide MILSATCOM at all latitudes and longitudes."[11] Because the DoD only occasionally has forces supporting national scientific and research activities in the South Polar Region and most operations are above 65 degrees south latitude, the threshold coverage requirement is stated as the "ability to provide MILSATCOM when/where needed in areas north of 65 degrees south latitude."[12] (But note that coverage of the North Polar Region is extremely important to the DoD.)

Capacity. *Capacity* as defined in the DoD MILSATCOM CRD encompasses both the kinds and amounts of *throughput* available, as well as the numbers of individual *accesses* to be supported by the system under specific terminal employment scenarios. Because the Joint Staff has already validated all quantitative requirements identified in the ERDB, the CRD uses this database as the baseline for the *capacity* KPP. Basically, the threshold requirement is to meet *known* quantitative capacity requirements as identified in the ERDB, and the objective requirement is to meet these threshold requirements "plus support projected growth rates."[13] The CRD recognizes the challenges in determining projected growth rates and caveats these quantitative requirements by pointing out that "DOD cannot accurately predict today precisely to the last data bit and user what MILSATCOM it will need – or can field – by 2010."[14] Further, many of the warfighting and support systems that will rely on MILSATCOM are still on the drawing boards and their information demands have not yet been quantified. The CRD thus recognizes that the ERDB is an estimate and states that as the ERDB is revised, subsequent updates to the CRD will capture those revisions.[15]

Because of the impossibility of predicting precise future capacity requirements, the CRD uses a "capabilities-based approach" to arrive at threshold and objective capacity requirements. The threshold capacity requirement is to "provide requisite amounts of *wideband and narrowband capabilities* (throughputs and accesses) to the warfighters and their supporting infrastructures."[16] With respect to wideband, the threshold requirement directs a "focus on deployed forces and OCONUS warrior support activities (e.g., Defense Information Systems Network, Diplomatic Telecommunications Service, intelligence community, etc.)."[17] With respect to narrowband, the threshold requirement is to "sustain UHF Follow-On (UFO) capabilities and augment with Mobile Satellite Services and Personal Communications Services," while the additional objective requirement is added to "support data rates up to 64 kbps into hand-held narrowband devices."[18]

Protection. For MILSATCOM systems, the DoD MILSATCOM CRD defines *protection* as "the system's ability to avoid, prevent, negate, or mitigate the degradation, disruption, denial, unauthorized access, or exploitation of communications services by adversaries or the environment."[19] Not all users require the same level of protection, and the DoD could not afford to provide the most stringent protection standards to all users and systems.

The CRD threshold requirement for the *protection* KPP is thus to "provide levels of protection to sub-sets of the overall MILSATCOM capacities."[20] Specifically, it defines the highest priority for protected services to be the *survivability* requirements for the National Command Authority and Single Integrated Operation Plan (SIOP) missions, followed by tactical warfighters who need *anti-jam* communications for their most vital command and control networks. Many Special Forces and other users require *low probability of intercept or detection (LPI/LPD)* capabilities. For sensitive diplomatic and intelligence activities, there is a vital threshold requirement for *U.S. control* of the communications path from end-to-end. Finally, there is a threshold requirement to "prevent unauthorized access to, or disclosure of, the information" that is carried by the MILSATCOM systems.[21]

The objective requirement for the *protection* KPP is to satisfy the threshold requirement "plus provide anti-jam, LPI/LPD and/or U.S. control for lower priority tactical, strategic, and supporting networks." Additionally, there is an objective requirement to "automatically detect, characterize, and neutralize offensive information operations."[22]

Access and Control. The CRD designates "*assured access*" as the most fundamental MILSATCOM need of the warfighter. "All the on-orbit capacity in the world is useless unless warfighters can access it, configure it, and use it to their best advantage."[23] As such, the *access and control* KPP includes the network management function, and is best measured by "the ability to dynamically provide the <u>right users</u>

access to the available MILSATCOM resources when and where they need it in accordance with the operational situation."[24]

The CRD identifies two objective requirements for the *access and control* KPP. The first is for "near-real-time authorization, denial, and preemption of access." The second is the ability to "accomplish dynamic resource configuration within a few minutes."

Each of these objective requirements has a corresponding threshold requirement that basically relaxes the timeframes for accomplishing these network management and allocation functions. For the first objective requirement, the corresponding threshold requirement is to provide the capability for CINCs and Joint Task Forces (JTF) to dictate resource utilization over apportioned resources and plan, allocate, and schedule access "within fractions of hours to a few hours." For the second, the threshold requirement is that MILSATCOM resources can be rapidly and dynamically configured and re-configured "within fractions of hours to no more than a few hours," with the caveat that this still be able to be done within minutes for selected networks.[25]

Interoperability. Recognizing that we will always fight as a joint (and usually combined) team, interoperability is absolutely necessary for ensuring unity of effort and synchronization of action. With respect to MILSATCOM systems, the CRD defines *interoperability* as "the ability of systems, units, or forces to provide information services to, and accept information services from, other systems, units, or forces and then to use the services so exchanged to enable them to operate effectively together."[26]

The two threshold requirements for the *interoperability* KPP are "interoperability between/among CINC and JTF components" and that MILSATCOM be "fully integrated as the space portion of the Defense Information Infrastructure." The CRD adds an objective requirement for "interoperability with allies and coalition partners and other Federal non-DoD agencies."[27]

Table 1 summarizes these threshold and objective requirements for the MILSATCOM key performance parameters.

Table 1. MILSATCOM Key Performance Parameters

PARAMETER	THRESHOLD	OBJECTIVE
COVERAGE	Ability to provide MILSATCOM when/where needed in areas north of 65 degrees south latitude.	Ability to provide MIL-SATCOM at all latitudes and longitudes.
CAPACITY	Provide requisite amounts of wideband and narrowband capabilities (throughputs and accesses) to the warfighters and their supporting infrastructures: -- Wideband (symmetric, asymmetric, and broadcast) Focus on deployed forces and OCONUS warrior support activities (e.g., DISN, DTS, intelligence community, etc.) -- Protected communications (see below) -- Narrowband (netted and other topologies) Sustain UFO capabilities & augment w/ MSS/PCS	Threshold plus support projected growth rates. Support data rates up to 64 KBPS into hand-held narrowband devices.
PROT'ECT'ION	Provide levels of protection to sub-sets of the overall MILSATCOM capacities: -- Survivable and anti-jam communications for NCA/SIOP forces -- Anti-jam for "front line" C2 and common-user networks -- LPI/LPD for critical tactical and strategic covert/sensitive users -- US Control for selected users (e.g., vital diplomatic and intelligence needs and selected tactical) Prevent unauthorized access to, or disclosure of, information.	Threshold plus provide AJ, LPI/LPD and/or US Control for lower priority tactical, strategic and supporting networks. Automatically detect, characterize, and neutralize offensive information operations.
ACCESS AND CONTROL	CINCs/Joint Task Forces dictate resource utilization over apportioned resources and can plan, allocate, and schedule access within fractions of hours to a few hours. MILSATCOM resources can be rapidly and dynamically configured and re-configured within fractions of hours to no more than a few hours (selected networks within minutes).	Near-real-time authorization, denial, preemption of access. Accomplish dynamic resource configuration within a few minutes.
INTER-OPERABILITY	Interoperability between/among CINC and JTF components (e.g, Land, Air, Naval, Mobility, Combat Support, and Special Operations Forces). MILSATCOM is fully integrated as the space portion of the DII.	Threshold plus inter-operability with allies and coalition partners and other Federal agencies (non-DoD).

Potential Role of Commercial Satellite Communications Systems

Upon analyzing the various capabilities emerging in the commercial sector as discussed in chapter two against the requirements of the Defense Department as discussed in this chapter, it is clear that there is a role for commercial systems. The

MILSATCOM CRD recognizes as much, and goes so far as to include "commercial services" under the umbrella of "MILSATCOM." In the executive summary to the CRD, it is stated that in order to satisfy tomorrow's needs, "warfighters will rely on a variety of MILSATCOM capabilities—encompassing both military systems and commercial services."[28] In his forward to the CRD, General Estes, Commander-In-Chief of US Space Command, states that it is "imperative we follow through on the acquisition programs and *commercial services*" (emphasis added) called out in the DoD Space Architect's MILSATCOM architecture.[29]

The key to recognizing the appropriate role for the commercial systems is a clear understanding of the DoD requirements discussed above. *Basically, it would appear that commercial capabilities can help satisfy quantitative requirements, but at a "cost" in most cases of accepting risk with respect to the qualitative requirements.* This, again, is evident in the CRD. Most favorable discussion of commercial services occurs in chapters that deal with *capacity*, while commercial shortcomings are evident when qualitative requirements are discussed (*protection*, and *access and control*, in particular).

Quantitative Benefits

Wideband needs represent the bulk of MILSATCOM capacity requirements.[30] Today, these are primarily satisfied by the Defense Satellite Communications System (DSCS), but DSCS is nearing the end of its useful life and its capacity falls far short of today's DoD requirements. Commercial capabilities can assist in reducing this shortfall in two ways.

First, as the ORD for the wideband replacement system is developed, the DoD will leverage "commercial-like" capabilities to the fullest extent possible to keep the replacement system affordable. The general philosophy in recent DoD requirements documents is to not allow requirements to drive DoD too far away from solutions that leverage commercial technology, components, and services. "Only in this way can DoD capture potential savings and satisfy as many requirements as possible."[31]

Second, the DoD can leverage the burgeoning "broadband-LEO" commercial systems. Based on currently projected growth rates for requirements, the DoD wideband replacement system, while providing significantly increased capacity, will still fall far short of meeting DoD capacity requirements. Growth in requirements is simply outpacing by a wide margin the growth in capacity provided by new technology. Until recently, the explosion in commercial SATCOM appeared focused in the "big-LEO" and "little-LEO" markets. But a review of Appendix A shows that many "broadband-LEO" systems are emerging that can be leveraged by DoD to help satisfy its growing wideband requirements.

Narrowband requirements likewise can be partially satisfied by commercial capabilities. The DoD MILSATCOM CRD recommends both increasing DoD-owned narrowband systems "while also embracing the new narrowband and mobile services being offered by the commercial SATCOM marketplace." It further states that, in the long term, "DoD should retain a military narrowband MILSATCOM capability with a possible improved objective system that leverages advances in commercial technology."[32]

Qualitative Risks

Commercial systems cannot be used, however, for all DoD users and requirements. The DoD will always have a requirement, for certain users and networks, for communications with a higher degree of *protection* than will be available from any commercial system. "DoD must provide adequate ***protected*** and assured MILSATCOM capacity to meet its most stringent and unique protected communications requirements, in both the mid-latitudes and North Polar Region" (emphasis in source).[33] There is very little debate about this requirement, "and it is not available today, nor likely tomorrow, except through DoD ownership."[34]

Even if this assertion proves untrue in the future and the commercial sector at some point provides adequately protected services, there are still some DoD communications that would be inappropriate for commercial systems. Those that are classified or extremely sensitive in nature require *U.S. and/or DoD control* of the system. Some uses of commercial systems are even *illegal* for the Defense Department.

The next chapter examines in greater depth these and many other risks and vulnerabilities associated with the use of commercial SATCOM systems.

Notes

[1] Department of Defense, *MILSATCOM Capstone Requirements Document (CRD)*, 24 April 1998, ES-3; on-line, Internet, 13 February 1999, available from http://www.laafb.af.mil/smc/mc/advanced_programs/adv_ehf/systemdef/requiremetns/protect_requirements/protect_requirements.htm.

[2] TRADOC Systems Manager for Satellite Communications, *The Army Satellite Communications (SATCOM) Architecture*, December 1998, 3-13.

[3] Ibid, 3-11.

[4] HQAF, *Program Management Directive for MILSATCOM*, 20 June 1994, 2.

[5] TRADOC Systems Manager for Satellite Communications, *The Army Satellite Communications (SATCOM) Architecture*, December 1998, 3-14.

[6] Ibid.

[7] Ibid, 3-10.

[8] DoD, *MILSATCOM CRD*, ES-1.

[9] Ibid, ES-1.

[10] Ibid, 1-18.

[11] Ibid, ES-4.

[12] Ibid, ES-4.

[13] Ibid, ES-4.

Notes

[14] Ibid, ES-6.
[15] Ibid, ES-6.
[16] Ibid, ES-4.
[17] Ibid, ES-4.
[18] Ibid, ES-4.
[19] Ibid, ES-5.
[20] Ibid, ES-5.
[21] Ibid, ES-5.
[22] Ibid, ES-4.
[23] Ibid, ES-8.
[24] Ibid, ES-8.
[25] Ibid, ES-4.
[26] Ibid, ES-8.
[27] Ibid, ES-4.
[28] Ibid, ES-2.
[29] Ibid, i.
[30] Ibid, ES-6.
[31] Ibid, ES-7.
[32] Ibid, ES-7.
[33] Ibid, ES-7.
[34] Ibid, ES-7.

Chapter 4

Commercial Satellite Communications Systems – Risks and Vulnerabilities

The *protection, control* and *legal issues* associated with the use of commercial SATCOM systems, identified at the end of the last chapter, merit further detailed discussion. Use of commercial systems poses many other risks and vulnerabilities, as well. The list of risk areas includes *access, cost, frequency management, equipment reliability,* and *interoperability*.

Protection

Commercial SATCOM systems represent a subset of our critical national infrastructure, the vulnerability of which is becoming increasingly recognized by national leadership:

"The infrastructures that gird and support the sinews of information-age society are unacceptably vulnerable to incidental, accidental and intentional disruption from terrorists, criminals, rogue states or peer adversaries. This weakness is so egregious it proffers the alluring, inexpensive and simple alternative of asymmetric strikes that could end run the world's most potent military power."[1]

The DoD recognizes the vulnerability of commercial SATCOM systems. Space and Missile Command (SMC) conducted a Military Integrated Satellite Communications

(MISC) study to evaluate the ability of commercial SATCOM systems to satisfy DoD requirements. While the study contains proprietary information and is not openly available, its key findings are available in a DoD Space Architect report. One conclusion from the study is that no commercial market is foreseen for protected or survivable communications services:

"None of the commercial systems are able to support the highly survivable, hardened requirements. Commercial systems are hardened for life extension in the space environment, however, they do not provide anti-scintillation protection. The studies also supported the assertion made by the military that commercial systems could not provide the required protected services. Although some commercial LEO systems do support polar regions, no protection is provided above encryption. Fixed services are all unprotected."[2]

Some question the conclusion that the commercial sector will *never* protect their services. As long as security, protection, and survivability are seen as uniquely military requirements, the DoD will most likely have to fund its own protection requirements, since the military comprises a shrinking portion of the commercial market.[3] But as threats to commercial systems not used by the military become more realistic, or if those non-military commercial systems are actually attacked at some point in time, some expect that the profit motive will drive commercial companies to invest in protection. A recent study of the vulnerabilities of commercial space systems concluded that the "motive" behind the system (military – "defense"; civil – "science"; commercial – "profit") impacts the extent to which vulnerabilities are protected. Civil systems, lacking both the profit motive of the commercial sector and the requirements driver of military systems, tend to be the least protected. But the study concludes that “the profit motive for the commercial side may be sufficient to protect against realistic threats,”[4] and that the proliferation of commercial systems in itself reduces their overall vulnerability by preventing the creation of a critical node.[5]

Others still believe that the DoD will foot the entire protection bill, even for purely commercial ventures not used by the military. General (Retired) Moorman, former Vice Chief of Staff of the Air Force, sees it in the historic context of military protection of commerce. Noting that navies were expanded in the 18th and 19th centuries to protect commerce and sea lines of communication, he states that “the military may be relied on to protect space lines of communication.”[6]

The bottom line is that it will take a partnership between DoD and private industry to begin protecting this infrastructure. In discussing President Clinton’s goal to provide significant infrastructure protection within five years, the head of the new Critical Infrastructure Assurance Office, Jeffrey Hunker, says:

“…almost all the critical infrastructure we are talking about is in private-sector hands. Even most Defense Department communications go over non-federally owned lines. So even if the federal government had a full court press in protecting critical infrastructure, we will fail unless we have the participation of the private sector.”[7]

A final dimension of the protection issue relates to the concept of “space control.” Space control is defined as “the means by which space superiority is gained and maintained to assure friendly forces can use the space environment while denying its use to the enemy.”[8] The newest release of our National Security Strategy recognizes that “space is essential for protecting U.S. national security, promoting our prosperity and ensuring our well-being in countless ways."[9] But in the sections on "Threats to U.S. Interests" and "Protecting Critical Infrastructures," space is not even mentioned. In fact, current DoD policy *does not permit* offensive counterspace actions that are necessary to establish space control.[10]

This disconnect between executive branch rhetoric on space control and its actual policies has been the focus of much recent attention in the national security community and Congress. In a recent decision brief on space control, the Center for Security Policy states that, given the National Security Strategy verbiage, "it is not only disingenuous but also irresponsible and outrageous that the Administration continues to oppose efforts to acquire *the means*" (emphasis in source) to accomplish space control.[11] U.S. Senator Bob Smith (R-NH) holds the Air Force as much responsible as the White House for the lack of coherence on space control, pointing out "Global Engagement" verbiage about the criticality of space control while the Air Force fails to allocate resources against the mission. He says that the Air Force "must truly step up to the spacepower mission" or Congress should consider creating a new separate Space Force.[12]

Control

As stated in the previous chapter, certain diplomatic, intelligence and other users require *U.S. control* over the entire path of their communications due to their sensitive nature. *U.S. control* means the system "is under the direct operational control of a corporate, private, or government activity that is subordinate—or immediately responsive—to the legal jurisdiction of US authority."[13]

A review of Appendix B reveals that many of the emerging commercial SATCOM systems are owned or governed by multinational consortiums representing a broad spectrum of countries, including China. Thus for certain users and networks, use of those particular commercial systems will be precluded. For all other users, those systems introduce risks and vulnerabilities that planners must carefully assess prior to making a decision to use them.

"SATCOM systems owned and operated by foreign governments, foreign corporations, or international consortiums may not always respond or act in a timely manner to US requests for service or continue to maintain already in-place service due to diplomatic, economic, social, or labor issues."[14]

Finally, the issue of *control* also extends to the *launch* function. While launch requirements are not addressed in the DoD MILSATCOM CRD, some consider "launch on demand" to be a valid DoD requirement. If it is, then this raises the question of whether there must be DoD owned and controlled launch capability, at a time when there is a strong push towards commercializing the launch function.

Legal Issues

One law expert sees public international law as facing its greatest challenge ever as information technology transforms international society. He argues that an entirely new theoretical structure of law will be required.[15] As information evolves into the target itself, the entire concept of warfare is revolutionized, and there is "a latent deficiency of public international law" addressing this area of future international conflict.[16] This new nature of warfare requires rethinking international law paradigms relative to the concepts of territory, aggression, and intervention.[17]

Specific examples with respect to commercial SATCOM services can be illustrated by examination of the International Maritime Satellite Organization (INMARSAT) satellite system. The purpose of INMARSAT is set forth in Article 3 of the INMARSAT Convention, where it is stated that the organization (INMARSAT) "shall act exclusively for peaceful purposes."[18]

The views of the DoD and COMSAT (an organization created by Congress in 1962, and the U.S. signatory to the INMARSAT Convention) differ from those of INMARSAT with respect to what constitutes "peaceful purposes." The DoD and COMSAT interpret peaceful use much more broadly than does INMARSAT. After U.S. Navy use of INMARSAT was publicized and challenged during Desert Storm, the Deputy Assistant Judge Advocate General, U.S. Navy, submitted a memorandum to the Chief of Naval Operations concluding that Navy units "may use INMARSAT in support of armed conflict under the auspices of U.N. resolutions."[19] Eleven days later, INMARSAT's Director General sent a letter to the U.S. Department of State challenging this broad interpretation of the INMARSAT Convention.[20] In 1993, the INMARSAT General Counsel's Office stated that, while peaceful purposes do not preclude military use, such use should generally encompass "distress and safety communications and other purposes recognized by international law."[21] The issue remains unresolved.

Other unresolved and/or untested legal issues include the applicability of "peaceful purposes" language in the Outer Space Treaty of 1967 relative to military communications via space; whether an attack on information legally constitutes an "act of war;" the legality of the use of *offensive* information warfare (for example, in counterattacking hacker attacks on information systems[22]); and a slew of others.

Other Risks and Vulnerabilities

Access

As identified in Chapter 3, *assured access* is the most fundamental warfighter MILSATCOM requirement. A corresponding fundamental risk in depending on commercial SATCOM is that the DoD generally has no guaranteed right of use. The military will compete with all other commercial customers. Equipment outages or system loading could deny military access with no recourse for reestablishing communications. Additionally, there is no "precedence" capability associated with commercial systems that would allow assured access for at least a subset of key users.

A second area relating to access is the issue of frequency "landing rights." The ability to use segments of frequency spectrum in foreign countries is not guaranteed, and must be approved by the host nation through a process that often requires large payments and many months lead time.

Also related to access is *coverage*. Many systems only provide access in small regions of the world (see **COVERAGE** column in Appendix A).

Another risk to assured access is the offensive counterspace capabilities of potential adversaries.[23] Of course this risk applies to military as well as commercial systems, but not equally. As discussed in the previous chapter, the military systems are far better protected.

A final access issue relates to the *number* of accesses possible in a given system. The density of military subscribers in small coverage "footprints" will saturate the capacity of some commercial systems. A related issue is the military requirement in many cases for "netted" services. Another limitation identified in the SMC MISC study is in this area of netted service. None of the commercial systems are designed to provide such service.[24]

Cost

Leasing commercial SATCOM services is not cheap. The SMC MISC study mentioned in Chapter 3 concluded that the life cycle costs of buying a SATCOM system were less than one-half the cost of leasing the same system.[25]

The Iridium system is illustrative and relevant since the DoD has invested in it. The cost for each telephone is around $2500.[26] An organization using forty Iridium telephones an average of three hours per day at a cost of $3 per minute would pay an annual bill of around $80 million. Such levels of Operations and Maintenance funding are not being programmed into Service budgets, and the Services are developing approval policies for acquisition of Iridium telephones in an effort to control costs.

Frequency Management Issues

In addition to the landing rights issues identified above, DoD development and acquisition timelines do not provide flexibility for quickly responding to changes in commercial market frequency trends. The fact that satellite hardware, once the satellite is launched, is nearly impossible to modify exacerbates the problem. For example, the DoD developed a “Tri-Band” satellite terminal capable of using the military X-band spectrum and the C and Ku commercial spectrum bands to enable DoD to leverage emerging commercial SATCOM systems. Well into the development cycle DoD recognized that the commercial market (as well as DoD’s new Global Broadcast Services) would be utilizing the commercial Ka-band far more so than the Ku-band, and expensive modifications to Tri-Band terminals are being considered.

Federal spectrum sell-offs (or in some cases, "give-aways") can further complicate matters. What is happening today in the civil spectrum with the Global Positioning System (GPS) can very well happen in the commercial spectrum with SATCOM: the loss of frequencies used by the military, causing expensive equipment replacements. (In the GPS case, DoD's Joint Tactical Information Distribution System – JTIDS – is being impacted as well.)[27]

Equipment Reliability

The most basic risk, relative to reliability of commercial equipment, is its vulnerability to the harsh environments in which the military operates. Very little unmodified commercial-off-the-shelf (COTS) meets DoD "ruggedization" standards, but some does. The Air Force is fielding a theater deployable communications package that is built from COTS modules procured from Motorola Corporation. Motorola's position is that "commercial hardware and software can withstand the heat and dust of the battlefield to continue functioning," which they claim was demonstrated during a recent COMBAT CHALLENGE Air Force exercise.[28]

A related reliability risk issue is the growing presence of contractors on the battlefield as the DoD depends increasingly on commercial systems. Contractors obligations and loyalties are to their company and stockholders. As non-combatants, they require additional allocation of scarce force protection resources. They are not trained for the emotional and physical hardships of the wartime environment, and can be a tremendous burden on warfighting units.[29]

Interoperability

Industry standards for several of the emerging commercial services in the big-LEO and little-LEO markets vary widely among service providers and from country to country. Virtually none of these new commercial SATCOM systems will interoperate with each other.

The broadband commercial systems lack transmission protocol standards. Most significantly, the Teledesic system, one of the most ambitious ventures with great potential utility to the DoD, will use its own proprietary protocol rather than Asynchronous Transfer Mode switching.[30]

Notes

[1] Col Alan D. Campen, USAF (Ret), "National Vulnerability Intensifies As Infrastructure Reliance Grows," *Signal*, July 1998, 20.

[2] DoD Space Architect, *MILSATCOM Final Report*, 1997, 4-32.

[3] Ben Iannotta, "Commercial Satellite Security: Who Pays?" *Defense News*, Sep 1998.

[4] Maj Sue B. Carter, *A Shot to the Space Brain: the Vulnerability of Command and Control of Non-Military Space Systems*, March 1997, 56.

[5] Ibid, 54.

[6] Robert Holzer, "Officials See U.S. Military Role As Commercial Space Protector," *Defense News*, Nov 1998.

[7] Jeffrey Hunker, quoted in George I. Seffers, "Defense Trends," *Army Times*, 12 October 1998, 30.

[8] USAF, "Space Operations," *Air Force Doctrine Document 2-2*, 23 August 1998, 8.

[9] The White House, *A National Security Strategy for a New Century*, October 1998, 25.

[10] The White House, *President Clinton Issues New National Space Policy*, 19 September 1996, n.p.; on-line, Internet, 18 November 1998, available from http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1996/9/20/1.text.1.

[11] Center for Security Policy, "The 'Gathering Storm': Will Clinton Persist in Ignoring Peril Arising from Emerging Threats to U.S. Control of Space?" *Decision Brief No. 98-D 180*, 5 Nov 98.

[12] U.S. Senator Bob Smith (R-NH), address to the Fletcher School/Institute for Foreign Policy Analysis Annual Conference, Cambridge, MA, 18 Nov 1998.

[13] Dept of Defense, *MILSATCOM Capstone Requirements Document (CRD)*, 24 April 1998, ES-6.

[14] Ibid, ES-5.

Notes

[15] Sean P. Kanuck, “Information Warfare: New Challenges for Public International Law,” *Harvard International Law Journal*, 37 (1996): 274.

[16] Ibid, 283.

[17] Ibid, 286-290.

[18] Richard A. Morgan, “Military Use of Commercial Communication Satellites: A New Look at the Outer Space Treaty and ‘Peaceful Purposes’,” *Journal of Air Law and Commerce*, 60 (Sep-Oct 1994): 282.

[19] Ibid, 294.

[20] Ibid, 295.

[21] Ibid, 286.

[22] George I. Seffers, “Thwarted hackers call Pentagon actions ‘offensive’,” “Defense Trends,” *Army Times*, 12 October 1998, 31.

[23] National Air Intelligence Center, *Threats to US Military Access to Space,* undated, inside front cover.

[24] DoD Space Architect, *MILSATCOM Final Report*, 1997, 4-32.

[25] Ibid, 4-31.

[26] LTC Gregg E. Peterson, *What Will Commercial Satellite Communications Do for the Military After Next?*, May 1998, 19.

[27] “White House Identifies Two New Signals for GPS,” *Inside the Air Force*, 18 Dec 1998.

[28] Clarence A. Robinson, Jr., “Commanders Gain Global Access through Commercial Equipment,” *Signal*, December 1998, 28.

[29] Maj Gen Norman E. Williams and Jon M. Schandelmeier, “Contractors on the Battlefield,” *Army*, January 1999, 34.

[30] Peterson, 19.

Chapter 5

Conclusions

The DoD will never have the resources, nor the requirement, to provide the most robust capabilities available in MILSATCOM systems to all its numerous users. It is clear, then, that DoD will *always* require commercial SATCOM systems to augment capacity. Whether the military's growing dependence on these commercial SATCOM systems is a strength or vulnerability will be determined by how well the "right mix" is achieved. Determining that right mix is a function of *clearly understanding* both DoD's requirements and the vulnerabilities and risks associated with a dependence on commercial systems. Basically, it would appear that commercial capabilities can help satisfy *quantitative* requirements, but at a "cost" in most cases of accepting risk with respect to the *qualitative* requirements.

As one industry analyst sees it, "commercial space and military space can be very complementary in the same way as commercial air and military air have and continue to be."[1] Essential to this approach is the use of commercial-off-the-shelf technology to the maximum extent possible; adopting best commercial practices; and emulating industry wherever practical.[2] As the SMC MISC study concluded:

> "The most promising DoD course of action is to buy a commercial satellite, modify the components to operate at a military allocated frequency band, and launch the satellite into a currently approved orbital location for military use. This system would provide the backbone of high

> capacity service at either X-band or Military Ka frequency, and be supplemented with a military unique system of EHF to provide survivable low data rate service and medium data rate protected service. Buying such a satellite system was shown to save in excess of 50 percent over the life-cycle cost of leasing transponders on commercial systems."[3]

As the requirement for the commercial sector to protect their communications continues to increase in the new Information Age, the blending of military and commercial interdependencies is accelerating.

> "In the early 21st century, two levels of satellite telecommunications appear to be emerging. A limited capacity, owned and operated by the military, will continue to service the need for highly protected and assured connectivity. The continued evolution and possible integration of legacy systems should fill this need. However, an increasing percentage of operational throughput and secure telecommunications needs will likely be provided by commercial or commercial-based USG owned or leased systems. As the commercial marketplace is increasingly driven to provide secure, tamper-resistant and interoperable capacity to meet the demands of the national and international marketplace, the military will soon recognize the opportunity to conduct information exchange with significantly fewer and less complex organic resources."[4]

The DoD needs to continue to partner with industry, as it has on the Iridium project with the development of a DoD gateway. The challenge for the DoD will be in determining how to "pick a winner" in the fiercely competitive environment that exists in the commercial marketplace both today and into the foreseeable future. But such partnerships are essential to reducing the vulnerability of our critical national infrastructures and enabling the DoD to achieve the "right mix" of future telecommunications systems.

Notes

[1] Dr. William A. Gaubatz (Director, Business Development, McDonnell Douglas Aerospace), "Space Sortie and Military Operational Space," *Specific Inputs to National Security Space Master Plan*, 7 June 1996, 6.

[2] LTG William H. Campbell, quoted in Robert K. Ackerman, "Army Information Experts Seek Commercial Solutions," *Signal*, June 1998, 41.

Notes

[3] DoD Space Architect, *MILSATCOM Final Report*, 1997, 4-32.

[4] Major General (USAF, Ret) William G. Jones, *White Paper on Space in the USAF*, undated, 11.

Appendix A

Commercial SATCOM Capabilities and Services[1]

SYSTEM	ORBIT	SATEL-LITES +spares	COVERAGE	SERVICES	AVAIL-ABILITY
AceS (Garuda)	GEO	2	SE Asia, India, China, Australia	V,MV,D,F, P	1999
ACTEL	GEO	Ph 1: 1 Ph 2: 2	Phase 1 = Zimbabwe, Zambia, Botswana, Namibia, Mozambique Phase 2 = All Africa	Ph 1: V,MV Ph 2: V,D	Ph1:NOW Ph2:01
Africom	GEO	1	Africa	MV	1999
AMSC	GEO	2	USA, Mexico, the Caribbean	V,MV,SMS, D,GPS	2000
APMT	GEO	2 + 1	SE Asia/China, Philippines, Vietnam	V,MV,F,D	2000
ASC	GEO	2	54 countries, from Turkey to Singapore and from Russia to Sri Lanka	V,F,D,Dm	1999?
Astrolink	GEO	5 + 4	Worldwide	Brdbnd,D	2001
Cyberstar	GEO	3	North America, Asia, Europe	Brdbnd,D	2000
Cyprus GEM	GEO	1	Europe, CIS countries, the Middle East, Africa	V,MV,D,F, Dm,SMS, GPS	2001
E-Sat	L-LEO	6	Mainly North America	SMS,Dm	2000
EAST	GEO	1	Saudi Arabia, East Europe, North Africa, South and West Africa	V,D, Brdbnd	2002
ECCO	B-LEO	46	Worldwide	V,MV,D,F, P	2001

Ellipso	B-LEO /MEO	10+1 LEO, 6 MEO	Primarily northern hemisphere to 55 degree S latitude	V, MV,D, F, P, GPS	2002
Expressway	GEO	14	Worldwide	Hi Speed D	?
FAISAT	L-LEO	32 + 6	Worldwide	D,Dm,SMS	2002
GE*Star	GEO	9	Americas, Europe, Asia, West Pacific, and Caribbean	Brdbnd, Vi	?
Gemnet	L-LEO	38	Worldwide	D,E,P	1999
Globalstar	B-LEO	48 + 8	70 degrees N to 70 degrees S latitudes	V, MV, F, P, SMS, GPS	1999
HALO	Pseudosat: aircraft at 52,000-60,000 ft.	100	Los Angeles and up to 200 other US West coast cities	Brdbnd	2000
ICO	MEO	10 + 2	Worldwide	MV,D,F, SMS	2000
Inmarsat	GEO	5	The 4 oceanic regions to 70 deg N&S lat and spotbeams for main land masses	MV,D,F, GPS	NOW
Iridium	B-LEO	66	Worldwide	V,D,F,P	NOW
KaStar	GEO	2	US, Central and South America, parts of Europe and Mexico	Brdbnd	2001
Leo-One	L-LEO	48	Worldwide	Dm, SMS, P, GPS	2000
M2A	GEO	1	Asia Pacific primarily Indonesia	V,D,F, Brdbnd,Vi	2000?
Movisat	GEO	3	Mexico, south US, Caribbean, Latin America	V, MV, SMS, GPS	NOW
MSAT	GEO	1	North and Central America	V,MV,F,D	NOW
Optus	GEO	2	Australia, PNG, NZ and Indonesia	V,MV,F,D, P	NOW
Orbcomm	L-LEO	48 + 8	Worldwide	SMS,E,F, GPS	NOW
Rostelesat	Brdbnd LEO/ MEO	91 LEO 24 MEO	Worldwide	Brdbnd, V, D	?
Satphone	GEO	3	Mid-East, N. Africa & the Mediterranean	V, MV	1999

Sky Station	Pseudosat: helium airships (at appr 22 km altitude)	250	Large metropolitan areas (as yet undesignated)	V, MV, Brdbnd	2000
SkyBridge	Brdbnd LEO	80	Worldwide	Vi,D,V	2001
Spaceway	GEO/MEO	8 GEO, 20MEO	All inhabited world except Asiatic Russia	V,D,Vi, Brdbnd	2002
Teledesic/ Celestri	Brdbnd LEO	288	Worldwide	Brdbnd, V	2002
Thuraya	GEO	2	Mid-East, Europe, Central Asia, North and Central Africa, Indian Subcontinent	V, MV, D, F, SMS	2000
VITAsat	L-LEO	2	Worldwide	D,E,SMS	NOW
WEST	GEO/ MEO	2 GEO, 9 MEO	Worldwide	Brdbnd	?

LEGEND: B-LEO = Big LEO (mainly voice/cellular)
Brdbnd = Broadband services
D = Data
Dm = Data Messaging
E = Email
F = Fax
GEO = Geosynchronous Earth Orbit
GPS = Global Positioning System
LEO = Low Earth Orbit
L-LEO = Little LEO (mainly low rate data/mobile data)
MEO = Middle Earth Orbit
MV = Mobile voice
P = Paging
SMS = Short Message Service
V = Fixed Voice
Vi = Video

ALTITUDES: LEO = up to 1,500 km MEO = 5,000 – 15,000 km GEO = 36,000 km

Notes

[1] All data in this table is extracted from Analysys Consultancy, *Analysys Satellite Communications Database*, 1998, n.p.; on-line, Internet, 18 January 1999, available from http://www.analysys.com/products/satellite/database.htm.

Appendix B

Commercial SATCOM Shareholders & Strategic Partners, and Market Strategies[1]

SYSTEM	SHAREHOLDERS & STRATEGIC PARTNERS	MARKET STRATEGY
AceS (Garuda)	Lockheed Martin,Pasifik Satelit Nusantara(PSN), Philippine Long Distance Co., Jasmine International PLC, Ericsson	ACeS aims to provide cost-effective, fill-in service for cellular operators and users. The main markets will be Indonesia and the Philippines. ACeS is proposing a tariff of USD1 per minute.
ACTEL	AMSC	Initially, ACTEL will serve sub-Saharan Africa where terrestrial networks are limited but will expand its service to the whole continent when its new satellite is launched.
Africom	Africom, Lockheed Martin	Africom wants to address the business market in sub-Saharan Africa which is currently under-served by terrestrial networks.
AMSC	Hughes, Ronald Baron, Singapore Telecom, AT&T	AMSC is targeting businesses that require remote communications and is now focusing particularly on narrowband mobile data. The second generation satellite may provide handheld mobile services. Airtime charges range from USD0.85 to USD1.99 per minute, depending on usage.
APMT	China Satellite Launch & Tracking Control General, China United Telecommunications Satellite Co. Ltd., China Telecommunication Broadcast Satellite, China Overseas Space Development & Investment Co., Singapore Technologies	The main market is expected to be in China (60%), with other countries in Southeast Asia also being targeted. The aim is to complement and extend terrestrial fixed and mobile coverage at low cost. APMT recently announced that its prices would be one third as high as rivals, such as Iridium, at around $1 per minute.

ASC	Essar Telecom, Essel Group, VSNL,Lockheed Martin	The key market for the first satellite is India, with the second satellite extending coverage across Africa. The aim is to complement and extend terrestrial coverage with low-cost mobile and fixed satellite services. Fixed trunking between Indian cities is also intended to be an important part of the market for the first satellite. The handheld phones are expected to cost USD700 to USD1000, offering international call at USD2 per minute.
Astrolink	Lockheed Martin, TRW	Lockheed plans to market the Astrolink service to businesses and common carrier providers worldwide, providing high-speed, two-way data services. Terminals are expected to sell at a few hundred US dollars.
Cyberstar	Loral Space & Communications, Alcatel Espace	Targeting broadband applications such as Internet and intranet access from low-cost fixed terminals. Loral has formed a strategic alliance with Alcatel to market the Cyberstar GEO and Skybridge LEO projects together.
Cyprus GEM	Cyprus Development Bank, Sumitomo Bank, OTE, Tele Danmark, Alenia, Hughes	It will offer capacity on a wholesale basis, at competitive price, to Telecom Operators.
E-Sat	Echostar Communications, DBSIndustries, Matra Marconi Space, SAIT	It is particularly targeting the gas and electricity utility industries in North America for remote monitoring of equipment for faults.
EAST	Matra Marconi Space, Digimed, Matra Hautes Technologies (France), Nera (Norway), Aon Space	Provides low cost services which complement and extend the coverage of terrestrial fixed and mobile services. For mobiles: Domestic charges will be about 60 cents per minute, falling to 30-40 cents. International surcharges will be 30-35 cents inside the EAST coverage area and 40-45 cents outside. For fixed: Domestic charges will be about 15cents per minute, falling to 10 cents. International surcharges will be 15 cents inside the EAST coverage area and 25 cents outside.
ECCO	Constellation Communications Inc., Orbital Sciences, Telebras, Bell Atlantic, Raytheon, Space Vest, Matra Marconi Space, CTA Launch Services Inc., E-Systems Inc.	ECCO is intended to provide complementary fixed and mobile services in rural areas. Brazil is one key market.

Ellipso	Mobile Communications Holdings, Vula Communications, Spectrum Networks System, Harris Corp., IAI (Israel Aircraft Industrie), Spectrum Astro Inc., L-3 Com, Lockheed Martin, Boeing, Aon Space	The main market is likely to be an extension of terrestrial mobile and fixed services to remote areas. Ellipso is proposing a tariff of USD0.35 (off peak) to USD0.50 per minute for mobile and fixed telephony, and a cost of around USD1000 for the terminal.
Expressway	GM Hughes Electronics	The service is aimed at businesses that send huge amounts of information around the world.
FAISAT	Final Analysis, Polyot Enterprises	Multiple market applications in the US and international markets. Phased deployment starting with non time-critical services and evolving to time-critical market and value-added services.
GE*Star	GE Americom	Offers broadband services, particularly to businesses worldwide. Main emphasis is on the US and European markets.
Gemnet	CTA Inc., Orbital Sciences	Target niche monitoring and tracking markets with low data requirements.
Globalstar	Space System/Loral, Qualcomm, DACOM, Dasa, Hyundai, Alcatel, France Telecom, China Telecom, Daimler Benz, Vodafone, Alenia Spazio, Elsag Bailey, Finmeccanica, Air Touch Communications, Ericsson	Globalstar aims to offer low-cost, high-quality services to areas currently under-served or not served at all by existing wireline and cellular telecommunications systems, particularly in developing countries. Each handheld terminal is expected to cost about USD750. Prices are expected to be in the range USD1.25 to USD1.50 per minute.
HALO	Wyman-Gordon, Raytheon Systems	The prices will be competitive with other offers such as T1 line.
ICO	BT, Deutsche Telecom, Telkom South Africa, Inmarsat, India’s VSNL, Hughes Electronic Corp.,Infonet, TRW, ICO Global Communications, unnamed Latin American partners	Target customers are domestic and international travelers, business and government organizations, commercial vehicles, maritime and aeronautical vessels, and residents of rural and remote areas. Customers will be served through a distribution chain of national wholesalers, resellers and retailers. The base tariff of calls will be USD1.95 per minute with a range from 50 cents to USD3 depending on the service used. The terminal will cost around USD700.

Inmarsat	Comsat (US), BT, Stratos Global, KPN, Telenor, OTE (Greece), Singapore Telecom, Telstra	Inmarsat-3: Main new product is Inmarsat mini-M, a notebook-sized telephone which can be used virtually anywhere in the world. This is targeted mainly at high-end users with a need to communicate in remote areas. End-user tariffs are around USD3 per min The phone costs about USD3000.
Iridium	Motorola, Nippon Iridium Corp., Vebacom GmbH, Sprint, BCD Mobile Communications Inc., STET, DDI, UCOM, SK Telecom Corp., PT Bakrie Communications Corp., Raytheon, Bouygues, Department of Defense	Business professionals are expected to be the main customers. It is also expected to be an invaluable tool for aeronautical and marine uses. Tariffs in the range USD1.1 to USD9 per minute are being proposed. Price of the Iridium/GSM handset is around USD3000.
KaStar	KaSTAR Satellite Communications Corp., Space Systems/Loral, Arianespace	Targeting broadband data services in North American markets.
Leo-One	dbX Corp.	Leo One will provide low-cost real-time, mobile and fixed service for industrial, business and personal data communications. Transceivers will cost USD100 to USD500. Service cost will be competitive with terrestrial-based data communication systems.
M2A	Pasifik Satelit Nusantara (PSN), Indosat	Provide consumer telecoms services as an adjunct to the public switched telephone network.
Movisat	Loral, Telefonica Autrey, Satelites Mexicanos SA, the Mexican Government	Target market is high end-users who need communications in remote areas. The phone is approximately briefcase sized.
MSAT	TMI Communications, Telesat Canada, GTIS, Glentel, Infosat, Mobility Canada Satellite	Targeting high end-users who need communications in remote areas. Its tariff is about USD1 to USD2 per minute. The phone is briefcase sized and costs approximately USD6000.
Optus	Optus Communications Pty Ltd.	Targeting use by government officials and others with need to communicate in remote areas. Current cost is AUD0.8 to AUD3.2 per minute for mobile voice services, with an AUD45-50 monthly fee. Briefcase sized terminals costing about AUD6000.

Orbcomm	Orbital Sciences Corp., Teleglobe Inc., Technology Resources Industries Bhd.	Orbcomm aims to provide high availability, low-cost, two-way, on-the-move communications over the entire globe. Personal users and remote monitoring are likely to be the key market segments. Currently, a handheld terminal costs USD1000.
Rostelesat	None for the moment	The project aims to be one of the world's biggest satellite provider of global fixed and broadband services.
Satphone	Lockheed Martin Telecommunications, Advanced Technology Fund Inc., M.O.Al Amoudi Corp.	Looking to complement and extend terrestrial fixed and mobile services.
Sky Station	NASA's Jet Propulsion Laboratory, Aerospatiale, Alenia, Finmeccania and United Solar Systems	Provide a cheap worldwide mobile phone and broadband data network. For example, the cost of a 2Mbps (burstable to 10 Mbps) internet channel should only be a few cents per minute.
SkyBridge	Alcatel Space, Loral Space & Communications, Mitsubishi, Sharp, Spar Aerospace (Canada), Aerospatiale (France), SRIW (Belgium), Toshiba, Com Dev(Canada)	It is primarily aimed at providing broadband access in areas with low or moderate density populations. Skybridge will be marketed together with Cyberstar. Loral and Alcatel have invested initially USD30 million in each other's system. Toshiba has also agreed to make an investment. Terminal cost is expected to be around USD700; access USD30 to USD40 per month.
Spaceway	Hughes Communications Inc.	Spaceway is expected to provide services in areas where the infrastructure is inadequate to meet the needs. The first target markets are likely to include North America. The terminals required are expected to cost about USD1000.
Teledesic/ Celestri	Bill Gates, Craig McCaw, Prince Alwaleed Bin Talal Bin AbdulAziz Alsaud (Saudi Arabia) Motorola, Boeing	It aims to provide broadband digital access at an affordable cost to information workers anywhere in the world from fixed terminals. Internet/intranet access are likely to be key markets.

Thuraya	Etisalat, Arabsat, BATELCO (Bahrain), ADIC, Al Murjan Trading & Industrial (Saudi Arabia), General Post & Telecom (Lybia), Q-Tel (Qatar), Dubai Investments, MTC (Kuwait), GIC (Kuwait), PTC (Yemen), Telecom Egypt, Nat. Telecom (Morocco), Tunis Telecom, DETECON (Germany), Hughes	Provide fixed and mobile services, which complement terrestrial services in remote areas. It is expected to cover the same geographical market as ASC's Agrani. Thuraya is aiming for an average price of USD0.50 per minute.
VITAsat	Volunteers in Technical Assistance, Final Analysis Inc., TOOL (Holland)	VITAsat will provide more reliable and cheaper access to health, education, disaster and other information in developing countries. VITA is a non-profit making organization.
WEST	Matra Marconi Space	The phased deployment of the hybrid constellation was aimed to match the growth rate and geographical pattern of the market. Terminal prices are expected to be in the range USD500 to USD2000.

Notes

[1] All data in this table is extracted from Analysys Consultancy, *Analysys Satellite Communications Database*, 1998, n.p.; on-line, Internet, 18 January 1999, available from http://www.analysys.com/products/satellite/database.htm.

Bibliography

Ackerman, Robert K. "Army Information Experts Seek Commercial Solutions." *Signal*, June 1998, 41-45.

Analysys Consultancy. *Analysys Satellite Communications Database,*1998, n.p. On-line. Internet, 18 January 1999. Available from http://www.analysys.com/products/satellite/database.htm.

Barrett, Lt Danelle. "Commercial Satellite Constellation Offers Potential Military Benfits." *Signal,* November 1998, 43-45.

Campen, Col (USAF, Ret) Alan D. "National Vulnerability Intensifies As Infrastructure Reliance Grows." *Signal*, July 1998, 20-22.

Carter, Maj Sue B. *A Shot to the Space Brain: The Vulnerability of Command and Control of Non-Military Space Systems*. Maxwell AFB, AL, Air Command and Staff College, March 1997.

Center for Security Policy. "The 'Gathering Storm': Will Clinton Persist in Ignoring Peril Arising from Emerging Threats to U.S. Control of Space?" *Decision Brief No. 98-D 180*, 5 Nov 98.

Dichman, Donald J. "The Constellations in LEO." *Launchspace*, Aug/Sep 1997: 40-41.

DoD Space Architect. *MILSATCOM Final Report*, 1997, 4-32.

Federal Aviation Administration. *1997 LEO Commercial Market Projections*. 25 July 1997.

Franklin, Larry. *An Analysis of the ORBCOMM Commercial Satellite System for Possible Military Use.* Monterey, CA, Naval Postgraduate School, June 1993.

Gaubatz, Dr. William A. "Space Sortie and Military Operational Space." *Specific Inputs to National Security Space Master Plan*, 7 June 1996.

Henry, Hugh A. *Military Satellite Communications Decision Support System Requirements Analysis and User Interface Design.* Monterey, CA, Naval Postgraduate School, June 1993.

Holzer, Robert. "Officials See U.S. Military Role as Commercial Space Protector." *Defense News*, 30 November 1998.

Houghtailing, Pamela. *Agencies Eye Commercial Birds as Interest in Satellites Grow,* 11 November 1996, n.p. On-line. Internet, 18 January 1999. Available from http://www.fcw.com/pubs/fcw/1111/feat.htm.

Hudgins-Bonafield, Christy. "Networking in the 21st Century, the Sky's the Limit." *Network Computing*, 15 March 1998, n.p. On-line. Internet, 18 January 1999. Available from http://www.techweb.com/se/directlink.cgi?nwc19980315s0017.

Iannotta, Ben. "Commercial Satellite Security: Who Pays?" *Defense News*, Sep 1998.

Jones, Major General (USAF, Ret) William G. *White Paper on Space in the USAF*, undated.

Kanuck, Sean P. “Information Warfare: New Challenges for Public International Law.” *Harvard International Law Journal*, 37 (1996): 272-292.

Knoth, Artur. “Space-Based Comms in the 21st Century.” *International Defense Review* 28 (May 1995): 63-65.

Morgan, Richard A. “Military Use of Commercial Communications Satellites: A New Look at the Outer Space Treaty and ‘Peaceful Purposes’.” *Journal of Air Law and Commerce* 60 (Sep-Oct 1994): 237-326.

National Air Intelligence Center, *Threats to US Military Access to Space,* Wright-Patterson AFB, OH, undated.

Petersen, LTC Gregg E. *What Will Commercial Satellite Communications Do for the Military After Next?* Carlisle Barracks, PA, U.S. Army War College, May 1998.

Rand Corporation. *U.S. Army Communications Using Commercial Satellites.* Santa Monica, CA, 1992.

Robinson, Clarence A., Jr., “Commanders Gain Global Access through Commercial Equipment.” *Signal*, December 1998, 25-28.

Seffers, George I. “Defense Trends.” *Army Times*, 12 October 1998, 30-31.

Smith, U.S. Senator Bob (R-NH). Address. Fletcher School/Institute for Foreign Policy Analysis Annual Conference, Cambridge, MA, 18 Nov 1998.

TRADOC Systems Manager for Satellite Communications. *The Army Satellite Communications (SATCOM) Architecture.* Fort Gordon, GA, December 1998.

The White House. *A National Security Strategy for a New Century.* Washington, D.C., October 1998.

The White House. *President Clinton Issues New National Space Policy*, 19 September 1996, n.p. On-line. Internet, 18 November 1998. Available from http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1996/9/20/1.text.1

U.S. Air Force. *Program Management Directive for Military Satellite Communications (MILSATCOM).* Washington, DC, 20 June 1994.

U.S. Air Force. “Space Operations.” *Air Force Doctrine Document 2-2,* 23 August 1998.

U.S. Army Signal School, Directorate of Combat Developments. *Warfighter Information Network: Personal Communications Systems.* Briefing. Fort Gordon, GA, March 1998.

U.S. General Accounting Office. *Military Satellite Communications: Opportunity to Save Billions of Dollars.* Washington, D.C., July 1993.

U.S. Space Command. *MILSATCOM Capstone Requirements Document (CRD),* 24 April 1998. n.p. On-line. Internet, 13 February 1999. Available from http://www.laafb.af.mil/smc/mc/advanced_programs/adv_ehf/systemdef/requiremetns/protect_requirements/protect_requirements.htm.

“White House Identifies Two New Signals for GPS,” *Inside the Air Force*, 18 Dec 1998.

Williams, Maj Gen Norman E., and Jon M. Schandelmeier. “Contractors on the Battlefield.” *Army*, January 1999, 32-35.

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air War College
Maxwell AFB, Al 36112